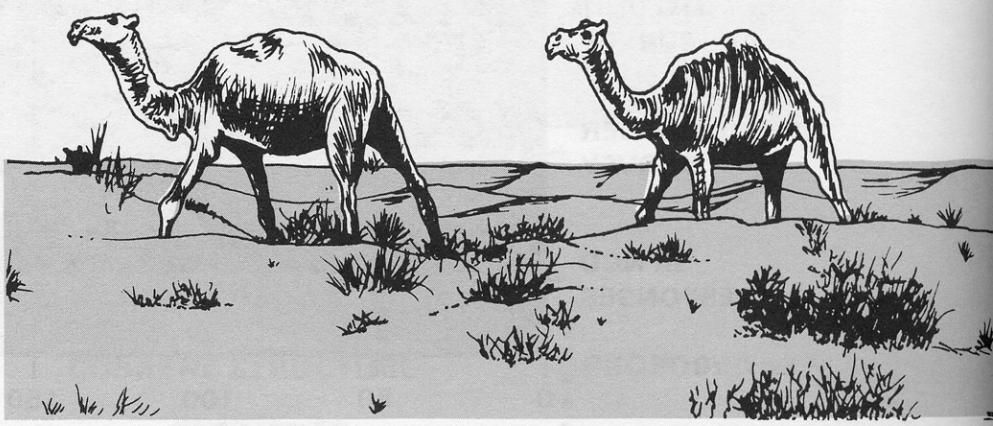
Hero of Desert Storm information systems

by Robert F. Weissert

Within six weeks of the Iraqi invasion of Kuwait, the U.S. Army Information Systems Command (ISC) had designed, installed and made fully operational a data communications architecture in Saudi Arabia using off-the-shelf commercial products.



Just as the Patriot missile became the hero of the Army's Desert Storm weapons systems, the Transmission Control Protocol/Internet Protocol (TCP/IP) became the Army's hero of Desert Storm's information systems.

Within six weeks of the Iraqi invasion of Kuwait, the U.S. Army Information Systems Command (ISC) had designed, installed and made fully operational a data communications architecture in Saudi Arabia using off-the-shelf commercial products.

The ISC, with a work force of some 40,000 soldiers and civilians operating in 14 nations and throughout the United States, is the largest military communications and automation organization in the world. The command, headquartered at Fort Huachuca, Ariz., has the mission to operate and maintain, engineer, acquire and install the systems which support the Army's information mission.

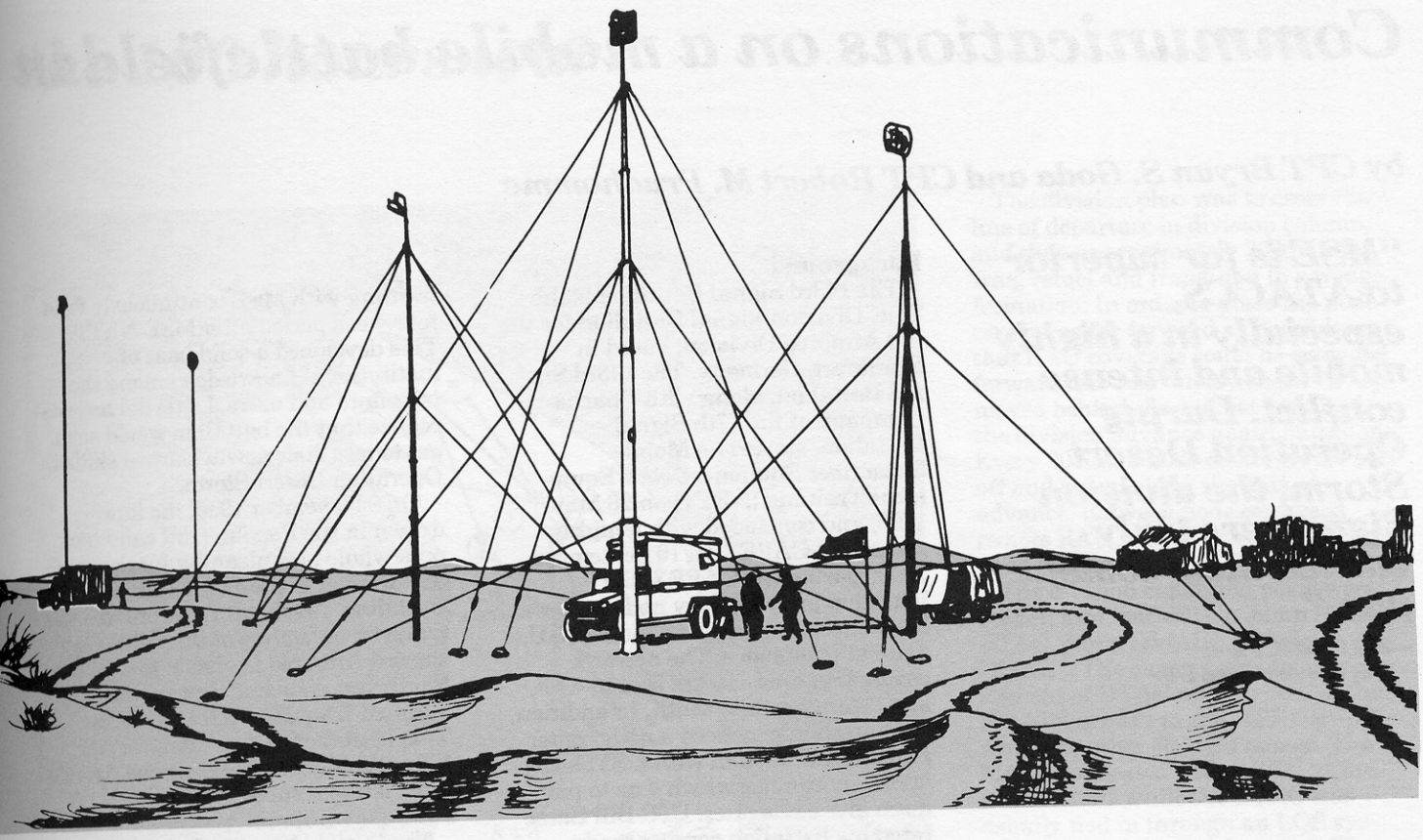
The heart and soul of this Operation Desert Storm network is TCP/IP which is the defacto open systems standard in the world today.

Since TCP/IP places the responsibility for session reliability and error correction on each individual host computer and not on the underlying networks, it proves to be the ideal solution for unstable battlefield conditions. Network management, trouble isolation and gateway configuration is accomplished remotely as the topology of the network changes with the tactical situation.

ISC, with the support of its engineering arm, the U.S. Army Information Systems Engineering Command, was able to install an "internet" environment consisting of over 20 subnetworks at key locations in Saudi Arabia.

The war is over now, but these systems will remain in operation for as long as needed to support troop redeployment.

Our ability to provide this service was predicated by our strategic commitment to employ reliable internet protocols worldwide. The installation of internet routers, gateways and terminal servers produced by Cisco Corporation of Menlo Park, Ca. provided the foundation for this architecture. Since these Cisco devices were already in the pipeline, we simply diverted them to Saudi Arabia.



Four years ago, ISC realized the benefit of fully supporting TCP/IP. This open systems protocol suite was installed on major Army processing centers which previously used IBM's SNA architecture. These systems include the Army personnel center, the Army finance center, the Army logistics centers and our regional data centers. All in all, the Army installed TCP/IP on over 1500 mini and mainframe computers worldwide.

When Desert Shield (the build-up phase of the war) placed an immediate requirement on the Army to move information quickly across the globe, ISC responded by providing an infrastructure that allowed interoperability between heterogeneous computer architectures over TCP/IP.

The Army's TCP/IP network in Saudi Arabia provides worldwide connectivity for all types of computers and operating systems. It is robust and dynamic enough to satisfy battlefield requirements for rapid change and it can be reconfigured in "real-time" as the situation changes. The network is designed to run IBM's 3270 protocol and other proprietary protocols over the TCP/IP channels.

Current users of the Army's Desert Storm network are experiencing throughputs in excess of 50 megabytes a day and interactive response time back to the United States of less than three seconds. This network is currently being used by Army, Navy, Air Force and Marine elements in Saudi Arabia.

This complex collection of routers, bridges, packet switches and satellite trunks requires tedious, constant and accurate network management from a centralized location. In 1988, the Commanding General of ISC directed his staff to investigate the use of "Rapid Prototyping" for strategic applications using fourth generation languages (4GL), artificial intelligence and computer aided software engineering tools (CASE).

One of the outcomes of that effort was the "Global Internet Information System." This UNIX based application was prototyped at the Cambridge Institute of Technology and was developed into a fully functional management tool by the Software Development Center at Fort Huachuca.

This tool is now being used to monitor 1500 Army computers on 56 heterogeneous networks around the world. Today, its primary focus is the Army networks and computers supporting Operation Desert Storm. This network management application not only monitors the operation of Army gateways, but can be used to reconfigure network parameters remotely.

This Saudi Arabian network system is centrally managed by the U.S. Army DDN Domain Manager, located on the east coast of the U.S. This Global Internet Information System is the "AWACS" of the Army internet, constantly watching all activity in its area.

CWO Weissert is a computer systems analyst assigned to the Deputy Chief of Staff for Operations, Headquarters, U.S. Army Information Systems Command. He currently serves as the Army's Internet Manager, responsible for the networking and interoperability of 1500 Army data communications at West Point and the U.S. Army Computer Science School. Before his assignment to ISC, Weissert was assigned to the White House Communications Agency in Washington, D.C.